

Información y computación cuántica*

Charles H. Bennett y David P. DiVincenzo

IBM Research Division, T. J. Watson Research Center, Yorktown Heights, New York 10598, USA

En el procesamiento de información, como en física, nuestra manera clásica de ver el mundo nos proporciona una aproximación incompleta a la realidad cuántica subyacente. Los efectos cuánticos como la interferencia y el entrelazamiento no juegan un papel directo en los métodos convencionales de procesamiento de información, pero pueden ser —hoy en teoría, pero a la larga en la práctica— utilizados para romper códigos, crear códigos irrompibles y acelerar computaciones que de otro modo serían intratables.

La teoría de la información y la computación ha experimentado un acelerón provocado por la aparición de una nueva rama y una renovación de sus conexiones históricas con la física básica, cuando se han extendido para abarcar el hasta entonces intacto territorio de la transmisión y el procesamiento de los estados cuánticos y la interacción de esta “información cuántica” con las formas tradicionales de información. Cabría preguntarse por qué esto no ha sucedido antes, puesto que hace mucho tiempo que los principios cuánticos se aceptaron como el fundamento de toda la física. Quizá los fundadores de la teoría de la información y la computación, como Shannon, Turing y von Neumann, estaban demasiado acostumbrados a pensar en el procesamiento de información en términos macroscópicos, al no tener todavía ante sí ejemplos tan convincentes como el código genético o la cada vez más pequeña microelectrónica. Sea como fuere, hasta hace poco se pensaba en la información en términos clásicos, y la mecánica cuántica jugaba sólo un papel secundario en el diseño de los equipos para procesarla y en el establecimiento de límites al ritmo con que se podía enviar por cierto tipo de canales. Ahora sabemos que una teoría completamente cuántica de la información y del procesamiento de la información nos ofrece, entre otras ventajas, un tipo de criptografía cuya seguridad descansa sobre principios fundamentales de la física, y la razonable esperanza de construir ordenadores cuánticos que podrían acelerar de forma espectacular la resolución de ciertos problemas matemáticos. Estas ventajas dependen de propiedades inconfundiblemente cuánticas como la incertidumbre, la interferencia y el entrelazamiento.

A un nivel más fundamental, ha quedado patente que una teoría de la información basada en los principios cuánticos amplía y completa la teoría clásica de la información, del mismo modo que los números complejos amplían y completan los reales. Además de las generalizaciones cuánticas de nociones clásicas como las de fuentes, canales y códigos, la nueva teoría incluye dos tipos complementarios de información cuantificable: la información clásica y el entrelazamiento cuántico. La información clásica puede copiarse a voluntad, pero sólo puede transmitirse hacia adelante en el tiempo, hacia un

receptor situado en el cono de luz futuro del emisor. Por el contrario, el entrelazamiento no puede copiarse, pero puede conectar dos puntos cualesquiera en el espacio-tiempo. Las operaciones convencionales de procesamiento de datos destruyen el entrelazamiento, pero las operaciones cuánticas pueden crearlo y usarlo para distintos propósitos, como acelerar determinadas computaciones clásicas o ayudar en la transmisión de información clásica o de estados cuánticos. Una parte de la nueva teoría de la información cuántica consiste en el estudio cualitativo y cuantitativo del entrelazamiento y de sus interacciones con la información clásica.

Algunos medios utilizados para transportar estados cuánticos de un lugar a otro y de manera más o menos intacta, como por ejemplo una fibra óptica, pueden verse como canales cuánticos. Al contrario que los canales clásicos, caracterizados por una única capacidad, los canales cuánticos tienen diversas capacidades distintas, dependiendo de para qué se estén tratando de usar y de qué otros recursos adicionales se pongan en juego.

Continúan descubriéndose nuevos efectos relacionados con la información cuántica, no sólo en áreas tradicionales de la computación, la capacidad de canales y la criptografía, sino también en áreas como la complejidad de la comunicación y la teoría de juegos.

I. TEORÍA DE DATOS CUÁNTICOS Y PROCESAMIENTO DE DATOS CUÁNTICOS

A. Datos cuánticos

¿En qué se diferencia entonces la información cuántica, y las operaciones que sobre ella pueden realizarse, de la información digital y las operaciones de procesamiento de datos convencionales? Un bit clásico (un elemento de memoria o un cable que lleve una señal binaria) es por lo general un sistema macroscópico, y se describe mediante uno o más parámetros continuos, como los voltajes. Dentro de este espacio de parámetros, el diseñador elige dos regiones claramente separadas para representar el 0 y el 1, y las señales son restauradas periódicamente a esas regiones típicas para prevenir que se pierdan a causa de las influencias del entorno, por la aparición de réplicas o debido a las tolerancias finitas en la manufactura. Una memoria de n bits puede estar en cualquiera de los 2^n

* *Nature* **404**, 247-255 (2000). Traducción y revisión: Adán Cabello, 2002.

estados, numerados de 000...0 hasta 111...1. Además de almacenar datos binarios, los ordenadores clásicos los manipulan; una secuencia de operaciones booleanas (por ejemplo, NOT y AND) actuando cada vez sobre uno o dos bits, es suficiente para realizar cualquier transformación determinista.

Por el contrario, un bit cuántico o “qubit” es típicamente un sistema microscópico, como un átomo, un espín nuclear o un fotón. Los estados booleanos 0 y 1 se representan por un par fijo de estados perfectamente distinguibles de un qubit (por ejemplo, las polarizaciones horizontal y vertical de un fotón: $|0\rangle = \leftrightarrow$, $|1\rangle = \updownarrow$). Un qubit también puede existir en un continuo de estados intermedios o “superposiciones”, representados matemáticamente por combinaciones lineales complejas de los estados base $|0\rangle$ y $|1\rangle$. Para fotones, estos estados intermedios corresponden a otras polarizaciones, por ejemplo $\nearrow = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $\swarrow = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, y $\circlearrowright = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$ (polarización circular a derechas). A diferencia de los estados intermedios de un bit clásico (como voltajes entre los valores standard 0 y 1), estos estados intermedios no pueden distinguirse de manera fidedigna de los estados base, ni siquiera en teoría. La superposición $\alpha|0\rangle + \beta|1\rangle$ se comporta frente a cualquier medida como $|0\rangle$ con probabilidad $|\alpha|^2$ y como $|1\rangle$ con probabilidad $|\beta|^2$. De manera más general, dos estados cuánticos pueden distinguirse de manera fidedigna si y sólo si sus representaciones vectoriales son ortogonales; por tanto, \leftrightarrow y \updownarrow pueden distinguirse de manera fidedigna mediante un tipo de medidas, y \nearrow y \swarrow mediante otro, pero ninguna medida puede distinguir de manera fidedigna \leftrightarrow de \nearrow .

Un par de qubits (por ejemplo, dos qubits en diferentes localizaciones) es capaz de estar en cuatro estados booleanos, $|00\rangle$, $|01\rangle$, $|10\rangle$ y $|11\rangle$, y también en cualquier superposición de ellos. Esto incluye estados como

$$\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle) = |0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \leftrightarrow \nearrow, \quad (1)$$

que puede describirse como producto tensorial de estados de los fotones individuales, y también estados como $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, que no admiten una descripción de ese tipo. Estos estados “entrelazados” corresponden a la situación en la cual ningún fotón por sí mismo tiene un estado definido, aún cuando el par sí lo tiene.

De manera más general, allí donde una cadena de n bits clásicos podía existir en uno de los 2^n estados booleanos $x = 000\dots 0$ hasta $111\dots 1$, una cadena de n qubits puede estar en cualquier estado de la forma

$$\Psi = \sum_{x=000\dots 0}^{111\dots 1} c_x |x\rangle, \quad (2)$$

donde c_x son números complejos tales que $\sum_x |c_x|^2 = 1$. En otras palabras, un estado cuántico de n qubits se representa por un vector complejo Ψ de longitud unidad en un espacio (“espacio de Hilbert”) de 2^n dimensiones,

una por cada posible estado clásico. La exponencialmente mayor dimensionalidad de este espacio distingue a los ordenadores cuánticos de los ordenadores clásicos analógicos, cuyo estado se describe mediante un número de parámetros que crece sólo linealmente con el tamaño del sistema. Esto es así porque los sistemas clásicos, tanto digitales como analógicos, pueden describirse completamente a partir de la descripción del estado de cada una de sus partes. Por el contrario, la inmensa mayoría de los estados cuánticos son entrelazados y no admiten una descripción de ese tipo. La capacidad de preservar y manipular estados entrelazados es la característica distintiva de los ordenadores cuánticos y es la responsable tanto de su potencia como de la dificultad para construirlos.

Un sistema cuántico aislado evoluciona de manera que se preservan las superposiciones y la distinguibilidad; una evolución de este tipo, llamada “unitaria”, es el análogo, en un espacio de Hilbert, de una rotación en el espacio real, y es otra diferencia importante entre los sistemas cuánticos y los analógicos. Evolución unitaria y superposición son los principios básicos de la mecánica cuántica.

B. Operaciones lógicas

Al igual que cualquier computación clásica se puede expresar como una secuencia de operaciones sobre uno o dos bits (por ejemplo las puertas lógicas NOT y AND), cualquier computación cuántica puede expresarse como una secuencia de puertas lógicas cuánticas sobre uno o dos qubits, esto es, operaciones unitarias que actúan sobre uno o dos qubits cada vez [1] (compárese con la Fig. 1). La puerta lógica más general sobre un qubit se describe por una matriz unitaria $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, que convierte $|0\rangle$ en $\alpha|0\rangle + \beta|1\rangle$ y $|1\rangle$ en $\gamma|0\rangle + \delta|1\rangle$. Las puertas lógicas sobre un qubit se pueden implementar físicamente de manera sencilla, por ejemplo mediante láminas de cuarto de onda y de media onda para fotones polarizados o mediante pulsos de radiofrecuencia para espines nucleares en un campo magnético.

La puerta lógica standard de dos qubits es la puerta controlled-NOT o XOR, que voltea su segundo input (u “objetivo”) si su primer input (o “control”) es $|1\rangle$, y no hace nada si el primer input es $|0\rangle$. En otras palabras, intercambia $|10\rangle$ y $|11\rangle$, y deja sin cambios $|00\rangle$ y $|01\rangle$. A diferencia de las puertas de un qubit, las puertas de dos qubits son difíciles de realizar en el laboratorio, porque requieren lograr que dos portadores de información cuántica que están separados sufran una interacción fuerte y controlada.

La puerta XOR es una interacción prototípica entre dos sistemas cuánticos, e ilustra varias características de la información cuántica, en particular la imposibilidad de clonar un estado cuántico desconocido, y la manera en que la interacción produce entrelazamiento. Si la XOR se aplica a datos booleanos en los que el segundo qubit es 0 y el primero 0 ó 1, el efecto es dejar el primer qubit sin cam-

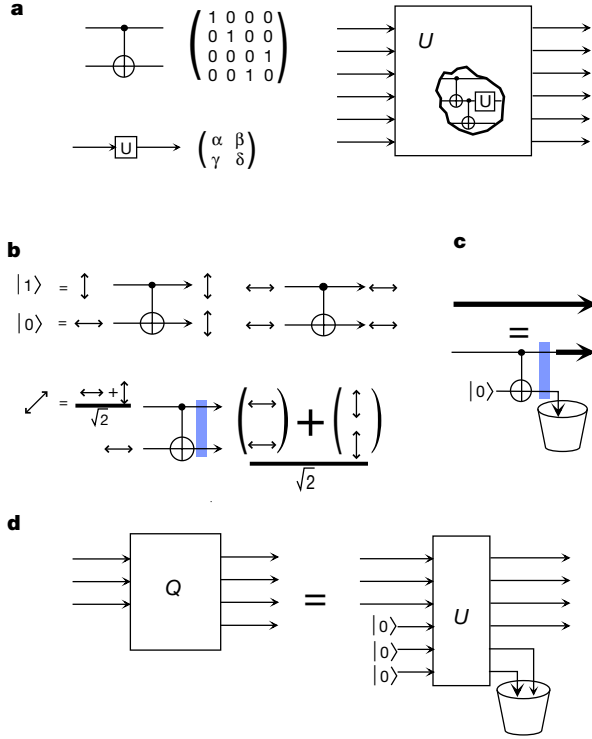


Figura 1: Operaciones lógicas cuánticas. **a**, Cualquier operación unitaria U sobre datos cuánticos puede sintetizarse usando la puerta lógica de dos qubits XOR, o controlled-NOT, y operaciones unitarias U sobre un qubit. **b**, La XOR actúa como un clonador clásico sobre inputs que tomen valores booleanos, pero si se trata de clonar valores intermedios, el clonado falla y se obtiene en su lugar un estado entrelazado (en azul). **c**, Un cable clásico (en línea gruesa) conduce de manera fidedigna 0 y 1, pero no superposiciones o estados entrelazados. Un cable clásico se puede definir como un cable cuántico que interactúa (via una XOR) con un qubit ancila 0 que después se descarta. **d**, El tratamiento más general, o superoperador, Q que puede aplicarse a datos cuánticos es una interacción unitaria con uno o más qubits 0, seguida de un descarte de algunos de los qubits. Los superoperadores son típicamente irreversibles.

bios, mientras que el segundo se convierte en una copia suya: $U_{\text{XOR}}|x, 0\rangle = |x, x\rangle$, para $x = 0$ ó 1 . Podría pensarse que la operación XOR también podría usarse para copiar superposiciones como $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, de manera que $U_{\text{XOR}}|\psi, 0\rangle$ diera $|\psi, \psi\rangle$, pero no es así. La unitariedad de la evolución cuántica requiere que la superposición de los estados input evolucione a la correspondiente superposición de outputs. Por lo tanto, el resultado de aplicar U_{XOR} a $|\psi, 0\rangle$ debe ser $\alpha|0, 0\rangle + \beta|1, 1\rangle$, un estado entrelazado en el que ningún qubit del output tiene por sí solo un estado definido. Si se pierde uno de los qubits del output (por ejemplo, se descarta o se permite que escape al entorno), entonces el otro se comporta como si hubiese adquirido un valor clásico aleatorio 0 (con probabilidad $|\alpha|^2$) ó 1 (con probabilidad $|\beta|^2$). Se perderá todo rastro de la superposición original $|\psi\rangle$, a menos que el output

perdido vuelva a entrar en juego. Este comportamiento no es sólo característico de la puerta XOR, sino de las interacciones unitarias en general; su efecto típico es convertir la mayoría de los estados no entrelazados iniciales de los sistemas que interactúan en estados finales entrelazados, lo que, desde el punto de vista de cada sistema, causa una perturbación impredecible.

C. Interacciones con el entorno

Dado que la física cuántica subyace en la física clásica, debe haber una forma de representar los datos y operaciones clásicos dentro del formalismo cuántico. Si un bit clásico es un qubit con el valor $|0\rangle$ ó $|1\rangle$, un cable clásico debe ser un cable que conduzca $|0\rangle$ y $|1\rangle$ de manera fidedigna, pero no superposiciones de ellos. Esto se puede implementar mediante la puerta XOR como se describió más arriba, con un $|0\rangle$ (que se descarta más tarde) en la posición objetivo. En otras palabras, desde el punto de vista de la información cuántica, la comunicación clásica es un proceso irreversible en el que la señal interacciona “en ruta” con el entorno, de manera que las señales booleanas pasan sin sufrir perturbaciones, pero otros estados sufren entrelazamiento con el entorno. Si el entorno se pierde o se descarta, la señal que sobrevive se comporta como si hubiese sido forzada de manera irreversible a elegir uno de los estados booleanos. No sólo un cable clásico, sino cualquier procesamiento clásico de datos, puede realizarse de manera similar mediante un procesamiento cuántico complementado por la interacción con un entorno cuántico que se descarta más tarde.

En la actualidad, paradójicamente, se piensa que las interacciones que entrelazan con el entorno son la principal razón por la cual el mundo macroscópico parece comportarse clásicamente y no cuánticamente [2]. Estados macroscópicamente diferentes —por ejemplo, los diferentes estados de carga que representan el 0 y el 1 en una célula de memoria VLSI (acrónimo inglés de “muy alta escala de integración”)—, sufren una interacción tan grande con el entorno que la información se encauza rápidamente hasta el estado en que está la célula. Por ello, incluso si fuese posible preparar la célula en una superposición de 0 y 1, la superposición evolucionaría rápidamente hacia un estado entrelazado complicado que incluiría el entorno, lo cual, desde el punto de vista de la célula, parecería una mezcla estadística de los dos valores clásicos, en lugar de una superposición. Este desmoronamiento espontáneo de superposiciones en mezclas se conoce como decoherencia.

El entrelazamiento con el entorno es por tanto un obstáculo muy importante para la computación cuántica. Para evitar que una computación cuántica sufra decoherencia y se convierta en una computación probabilística clásica (que podría hacerse también con un ordenador clásico), es necesario tanto crear y mantener el entrelazamiento entre los grados de libertad computacionales, como evitar el entrelazamiento entre estos y el entorno. Hasta hace poco tiempo parecía que el número de pasos

factibles en una computación cuántica coherente debería ser menor que el cociente entre el tiempo de decoherencia y el tiempo de encendido-apagado τ_d/τ_s característico de los sistemas cuánticos elementales que se usen en el hardware. Incluso en caso de que todos los demás problemas en el diseño de un ordenador cuántico práctico pudieran superarse, los valores que se obtienen actualmente para τ_d/τ_s no son lo suficientemente elevados para hacer que los ordenadores cuánticos fuesen competitivos frente a los clásicos; además, la búsqueda de sistemas con valores de τ_d/τ_s mayores podría quedar finalmente bloqueada por las propiedades fundamentales de los átomos y núcleos disponibles. Aparte de la decoherencia, también parecía que las operaciones de una sola puerta lógica tendrían que hacerse más y más precisas cuanto más larga fuese la computación.

Gran parte de este pesimismo se ha disipado tras el descubrimiento de la computación cuántica tolerante a fallos (CCTF), el análogo cuántico del descubrimiento de von Neumann de que para hacer cálculos clásicos arbitrariamente largos de manera fidedigna pueden usarse puertas lógicas clásicas no fidedignas, suponiendo que la probabilidad de error por puerta lógica es menor que un cierto valor umbral constante. Gracias a la CCTF, parece que los investigadores experimentales “sólo” necesitan construir un hardware cuántico que tenga una decoherencia por puerta lógica por debajo de un umbral finito (que se estima entre 10^{-6} y 10^{-2} , con una precisión similar para las rotaciones de una puerta lógica), para que los ordenadores cuánticos pudiesen hacer cálculos arbitrariamente complejos.

Tras esta introducción, pasamos a repasar cuáles son los principales paralelismos y diferencias entre el procesamiento de información cuántica y clásica.

D. Aceleración cuántica de una computación clásica

Potencialmente, esta es la aplicación más importante del procesamiento cuántico de datos. Usando puertas lógicas y cables cuánticos, con estados entrelazados fluyendo a través de ellos en los estadios intermedios de la computación, ciertas computaciones que relacionan inputs clásicos x con outputs clásicos $f(x)$, pueden hacerse en un menor número de pasos que en cualquier otra secuencia conocida de puertas lógicas clásicas. Lo que ha tenido mayor repercusión es que un ordenador cuántico puede factorizar números enteros grandes en un tiempo que es polinómico en el logaritmo del mejor de los tiempos clásicos [4, 5], amenazando de este modo la seguridad de los criptosistemas basados en la presumible dificultad de factorizar. Esta aceleración exponencial depende de la capacidad que tenga un ordenador cuántico para paralelizar masivamente el cálculo de una transformada de Fourier, usando interferencias destructivas entre varios caminos computacionales paralelos, capacidad que crece de forma exponencial con el número de qu-

bits físicos involucrados en la computación. Otro tipo de problemas en los que los ordenadores cuánticos parecen proporcionar aceleraciones exponenciales es el de la simulación de sistemas cuánticos de muchas partículas [6, 7]. En contraste con estos problemas bastante especializados, existe otra clase mucho más amplia de problemas que puede acelerarse cuadráticamente, esto es, resolverse en un tiempo proporcional a la raíz cuadrada del tiempo que requeriría un ordenador clásico. Entre ellos figuran los problemas de búsqueda y optimización (por ejemplo, dado un algoritmo para calcular la función F , encontrar el input s para el que $F(s) = 0$, o un input para el que $F(s)$ es mínimo) [8, 9]. Para otros problemas no hay aceleración cuántica. Entre ellos, la evaluación de funciones iteradas [10, 11] (por ejemplo, dado un algoritmo para calcular F , calcular la iteración n -ésima $F^{(n)} = F(F(F(\dots(.)) \dots))$ para un n grande) o el cálculo de la paridad de un conjunto aleatorio [12, 13].

E. Teoría cuántica de la información

Esta teoría generaliza las nociones clásicas de fuente y canal y las técnicas relacionadas de codificación de la fuente y el canal, y, al mismo tiempo, introduce un nuevo recurso, el entrelazamiento, que interacciona con la información clásica y cuántica en una variedad de formas que no tienen un análogo clásico.

Como dijimos antes, los canales cuánticos tienen distintas capacidades, dependiendo de para qué se usen y de qué recursos auxiliares se empleen. Entre otras incluyen las siguientes:

Capacidad clásica, C , es igual a la velocidad máxima de transmisión de manera fidedigna de bits clásicos por el canal;

Capacidad cuántica, Q , es la velocidad máxima de transmisión de manera fidedigna de qubits intactos por el canal;

Capacidad cuántica asistida clásicamente, Q_2 , se define como la velocidad máxima de transmisión de manera fidedigna de qubits por el canal, con la ayuda de una cantidad ilimitada de comunicación clásica, en ambos sentidos, entre el emisor y el receptor; y

Capacidad clásica asistida por entrelazamiento, C_E , se define como la velocidad máxima de transmisión de bits clásicos por el canal, con la ayuda de una cantidad ilimitada de entrelazamiento previo entre el emisor y el receptor.

Para todos los canales conocidos, estas capacidades satisfacen la relación $Q \leq Q_2 \leq C \leq C_E$, pero parece ser que varían independientemente y no son fáciles de calcular a partir de los parámetros del canal cuántico. De nuevo sucede lo contrario de lo que ocurre con la capacidad de los canales clásicos.

F. Compresión cuántica de datos y corrección de errores

Las dos técnicas centrales de la teoría clásica de la información, la codificación de fuentes y la codificación de canales, tienen análogos cuánticos directos. Una fuente cuántica es una entidad que emite estados cuánticos ψ_i con probabilidades p_i , y un canal es una entidad, como una fibra óptica, que transmite estados cuánticos de manera más o menos fidedigna entre un emisor y un receptor.

La entropía de von Neumann de una fuente cuántica, $S = -\text{Tr} \rho \log_2 \rho$, donde $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$, determina el número mínimo de qubits en el que, asintóticamente, pueden comprimirse las señales de la fuente mediante un codificador cuántico de manera que puedan ser recuperadas de manera fidedigna mediante un descodificador cuántico. Esto es el equivalente de la compresión clásica de datos o codificación de la fuente, mediante la cual la información clásica redundante se comprime y es recuperada de manera fidedigna. Sin embargo, la compresión de datos cuánticos [14] difiere en que puede aplicarse a estados no-ortogonales (por ejemplo, fotones horizontales y diagonales, como se muestra en la Fig. 2a), que se echarían a perder si uno tratase de comprimirlos clásicamente. También ocurre que, como los estados son no-ortogonales, si lo que se pretende es reconstruirlos de manera fidedigna al final de la recepción, el codificador no puede guardar copia, ni siquiera un recuerdo, de ellos. Un codificador cuántico es como un telegrafista discreto que transmite los mensajes sin recordarlos.

La codificación de la fuente elimina la redundancia, permitiendo que los datos se envíen de manera más eficiente a través de un canal sin ruido. Por el contrario, la corrección de errores o codificación del canal introduce redundancia para permitir que los datos resistan la transmisión a través de un canal con ruido. El código clásico de corrección de errores más sencillo es el código de triple repetición $0 \rightarrow 000$, $1 \rightarrow 111$, que permite que los bits codificados sean recuperados de manera fidedigna incluso tras, como mucho, un error en la transmisión del código de tres bits. Para datos cuánticos existen códigos de corrección de errores equivalentes, pero requieren más redundancia porque necesitan proteger no sólo estados booleanos, sino también cualquier superposición arbitraria de los mismos [15–20]. El código cuántico de corrección de errores más sencillo (Fig. 2b) codifica un qubit input arbitrario $|\psi\rangle$ en un estado entrelazado de cinco qubits de manera que, si cualquiera de ellos se corrompe *en vuelo*, el descodificador puede canalizar los efectos del error en los cuatro qubits suplementarios (llamados ancillas), devolviendo así al primer qubit a su estado original. La capacidad cuántica Q de un canal con ruido puede definirse, de manera análoga a la capacidad clásica, como el máximo cociente entre el número de qubits transmitidos de manera fidedigna y el número de bits transmitidos usando un canal con ruido al usar códigos cuánticos de corrección de errores. Esta capacidad cuántica

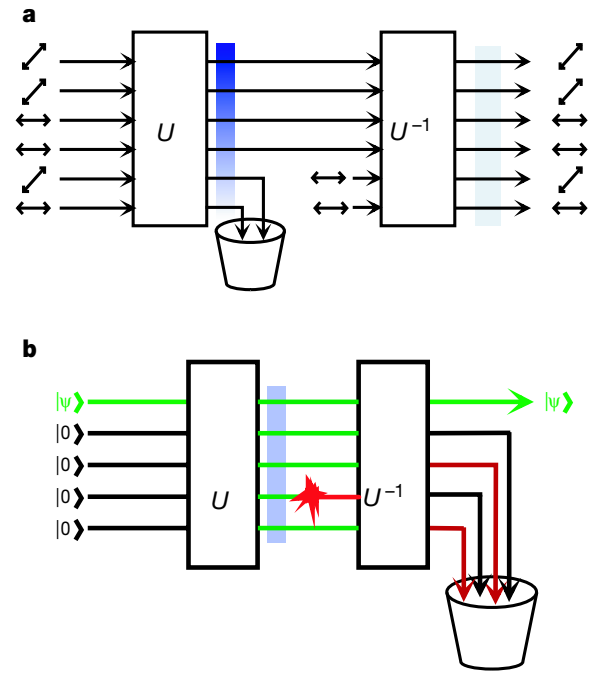


Figura 2: Compresión de datos cuánticos y corrección de errores. **a**, En la compresión de datos cuánticos, los inputs de una fuente redundante (aquí una secuencia desconocida de fotones horizontales y diagonales) se transforman unitariamente en un estado entrelazado (en azul) en el que casi toda la información se ha concentrado en algunos de los fotones, lo que permite descartar los otros. Al final del canal, los fotones que se han descartado se reemplazan por fotones standard (horizontales) y se deshace la transformación unitaria, lo que da como resultado una muy buena aproximación al estado original. **b**, Un código cuántico de corrección de errores con un codificador y descodificador unitario. Un qubit entrante arbitrario $|\psi\rangle$ se entrelaza con cuatro qubits $|0\rangle$ standard de manera que si uno cualquiera de los cinco qubits se estropea, el descodificador todavía puede restaurar exactamente el estado original.

es normalmente inferior, y nunca puede ser mayor, que la capacidad C para transmitir bits clásicos de ese canal. La desigualdad $Q \leq C$ se cumple para todos los canales, porque si un canal puede transmitir de manera fidedigna un qubit, entonces también podría transmitir los qubits particulares $|0\rangle$ y $|1\rangle$.

El descubrimiento en 1995 de los códigos cuánticos de corrección de errores supuso una gran sorpresa, probablemente porque la gente estaba acostumbrada a pensar en la corrección clásica de errores en un lenguaje no apropiado para su generalización cuántica. Por ejemplo, la triple repetición, si se entiende que quiere decir hacer tres copias del qubit input ($\psi \rightarrow \psi \otimes \psi \otimes \psi$), choca con la bien conocida imposibilidad de copiar exactamente (“clonar”) un estado cuántico desconocido. Retrospectivamente, la generalización cuántica natural de la triple repetición puede verse como la aplicación $\alpha|0\rangle + \beta|1\rangle \rightarrow \alpha|000\rangle + \beta|111\rangle$, que no viola ningún principio cuántico y, de hecho, basta

para corregir errores de un único qubit en cualquier input booleano. Como dijimos antes, son necesarios dos qubits más de redundancia para extender la protección a inputs no-boleanos. Aunque tienen una estructura análoga a la de los códigos clásicos de corrección de errores discretos, los códigos cuánticos de corrección de errores poseen la notable capacidad de proteger un continuo de inputs de un continuo de errores. Por ejemplo, en la Fig. 2b, el qubit input podría ser un fotón en cualquier estado de polarización, y el error (en rojo) podría ser una rotación arbitraria de la polarización de uno de los cinco qubits que van por el canal; en cualquier caso, el error podría corregirse. Este es el lado beneficioso de la linealidad de la mecánica cuántica: si un código cuántico de corrección de errores protege un conjunto discreto de inputs lo suficientemente rico de un conjunto discreto de procesos de error lo suficientemente rico, entonces también protegerá cualquier superposición de esos inputs de cualquier superposición de esos errores. Además de las capacidades C y Q , los canales cuánticos tienen capacidades Q_2 y C_E mencionadas más arriba, de las que hablaremos más adelante.

La rama más antigua de la teoría cuántica de la información [21–23] tiene que ver con el uso de canales cuánticos para la transmisión de información clásica. Para los canales cuánticos no es fácil calcular ni siquiera la aparentemente prosaica capacidad C , ya que puede depender de que se use un codificador cuántico para preparar inputs entrelazados con múltiples usos del canal, y/o un descodificador cuántico para hacer medidas coherentes sobre múltiples outputs del canal. Al contrario que cualquier canal clásico, algunos canales cuánticos son superaditivos en el sentido de que se puede enviar más información clásica a través de n canales usados en paralelo que la que se puede enviar usando n veces el mismo canal [24–28].

G. Comunicación asistida por entrelazamiento

Dos formas de transmisión cuántica de información que no tienen contrapartida clásica, pero que están íntimamente relacionadas entre sí, son la teleportación cuántica [29] (Fig. 3a) y la codificación cuántica superdensa [30] (Fig. 2b). En ambas hay un paso inicial en el que dos partes comparten un par de partículas preparadas en un estado máximamente entrelazado como $\sqrt{\frac{1}{2}}(|00\rangle + |11\rangle)$ (a menudo llamado par de Einstein-Podolsky-Rosen o EPR), seguido de un segundo paso en el que este entrelazamiento compartido se usa para transmitir un qubit mediante dos bits clásicos (en la teleportación), o transmitir dos bits clásicos mediante un qubit (en la codificación superdensa). La teleportación cuántica ilustra el hecho de que la transmisión de estados cuánticos intactos requiere dos tipos de recursos cualitativamente diferentes: un recurso cuántico que no puede clonarse, y un recurso dirigido que no puede viajar más rápido que la luz. En la transmisión directa de un qubit, ambas funciones son

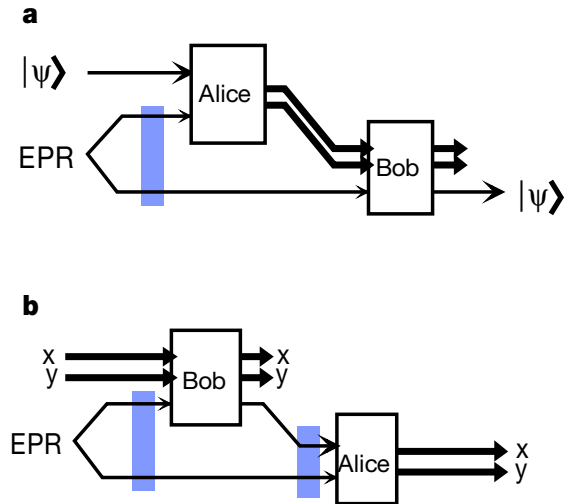


Figura 3: Transmisión de información cuántica entre un emisor (Alice) y un receptor (Bob). **a**, En la teleportación cuántica, compartir previamente un par EPR y transmitir un mensaje clásico de dos bits de Alice a Bob, es suficiente para transmitir un estado cuántico desconocido, incluso cuando no está disponible un canal cuántico directo entre Alice y Bob. **b**, En la codificación cuántica densa, compartir previamente un par EPR y transmitir un único qubit de Alice a Bob, es suficiente para transmitir un mensaje clásico arbitrario de dos bits (x, y) .

desempeñadas por la misma partícula. En la teleportación, la primera función es desempeñada por el par EPR compartido, y la segunda por los dos bits clásicos. Esta situación se puede resumir diciendo que la teoría clásica de la información trata de una clase de información y una clase de primitiva de comunicación sin ruido (la transmisión de un bit), mientras que la teoría cuántica de la información trata de dos clases (la información clásica y el entrelazamiento), y tres primitivas (transmitir un bit, transmitir un qubit y compartir un par EPR), que están relacionadas mediante la codificación superdensa y la teleportación.

La codificación densa (Fig. 3b) es un ejemplo de comunicación asistida por entrelazamiento, y muestra que para un canal sin ruido de un qubit, $C_E = 2$, mientras que $C = Q = 1$. Sorprendentemente, el cociente C_E/C aumenta típicamente con el ruido y, de hecho, puede alcanzar valores arbitrariamente grandes para canales que sean tan ruidosos que las capacidades cuánticas Q y Q_2 se hagan cero [31]. Por consiguiente, al contrario que la mayoría de los efectos cuánticos, la mejora mediante el entrelazamiento de la capacidad clásica del canal clásico no desaparece en el límite de mucho ruido. En este aspecto, esto recuerda a la habilidad que tienen los sistemas grandes de resonancia magnética nuclear para llevar a cabo computaciones cuánticas no triviales y, al mismo tiempo, estar cerca del equilibrio térmico.

Recientemente, la codificación superdensa y la telepor-

tación han recibido mucha atención experimental. El primer trabajo se debe al grupo de Innsbruck [32], que implementó una versión de la codificación superdensa en la que tres estados distinguibles (en lugar del máximo teórico de cuatro) son creados manipulando un miembro de un par de fotones entrelazados en polarización. El mismo grupo experimental logró la teleportación usando esos estados de fotones [33]. Utilizando estas técnicas ha sido posible lograr otros protocolos relacionados con el entrelazamiento; por ejemplo, la creación de entrelazamiento entre tres partículas. En Roma [34] se ha implementado una aproximación experimental diferente, en la que se teleporta otro atributo de uno de los fotones EPR (como la posición). Este experimento es más sencillo, ya que involucra a dos fotones en lugar de tres. Otro experimento muy reciente [35], que ha seguido más fielmente la versión del esquema de teleportación sugerida por Vaidman [36], en la que se teleportan grados de libertad cuánticos continuos, demuestra que un estado cuántico arbitrario de un modo óptico puede teleportarse con un alto grado de fidelidad. Teniendo en cuenta las limitaciones en la intensidad del modo, lo que se está manejando es un sistema con aproximadamente un millón de estados, en contraste con los sistemas con dos estados que se usaban en los trabajos anteriores. Por último, se ha conseguido realizar las operaciones necesarias para teleportar un estado de un espín nuclear usando resonancia magnética nuclear [37], pero la teleportación tiene lugar a la distancia de una molécula.

Aunque el entrelazamiento no se puede usar por sí solo para transmitir mensajes clásicos, sí que puede reducir la cantidad de comunicación clásica necesaria para hacer computación distribuida [13, 38, 39]. Clásicamente, la “complejidad de la comunicación” es la cantidad de comunicación necesaria para evaluar una función con varios inputs en lugares remotos. Por ejemplo, si Alicia y Bob tienen cada uno de ellos una agenda de citas con n huecos libres, entonces son necesarios $O(n)$ bits de comunicación para determinar si hay alguna hora a la que los dos estén libres. Si se les permite compartir previamente entrelazamiento, o si se les permite comunicarse mediante qubits en lugar de mediante bits, la complejidad de la comunicación en este problema se reduce de $O(n)$ a $O(\sqrt{n} \log n)$.

H. Cuantificar y destilar entrelazamiento

Debido a su utilidad en protocolos como la teleportación, es importante disponer de medidas cuantitativas del entrelazamiento, y averiguar si todos los estados entrelazados (aquellos no expresables como productos de estados de sus partes, o mezclas probabilísticas de tales productos) pueden convertirse en pares EPR y, si es así, con cuánta eficiencia puede hacerse. En el caso de estados puros bipartitos, el entrelazamiento se mide de manera natural mediante la entropía de entrelazamiento del estado, que es la entropía de von Neumann de cualquiera de sus subsistemas. Para tales estados [40–42], la entropía

de entrelazamiento $E(\Psi)$ es igual tanto a la entropía de formación —el número de pares EPR necesarios asintóticamente para preparar un ejemplar del estado mediante comunicación clásica y operaciones locales—, como a su entrelazamiento destilable —el número de pares EPR puros que se pueden preparar asintóticamente a partir de un ejemplar del estado, mediante comunicación clásica y operaciones locales—.

Para estados mezcla y estados de tres o más partículas, la situación es más complicada, y hay varias formas no equivalentes de entrelazamiento. Se han estudiado estados de muchas partículas, tanto puros como mezcla [43–45]. Los estados mezcla, por lo general, tienen un entrelazamiento destilable que es menor que su entrelazamiento de formación, lo que refleja la irreversibilidad del proceso de mezcla. Una forma extrema de este fenómeno es la existencia de los llamados estados con entrelazamiento “atado” (“bound”) [46] —estados mezcla que son entrelazados, pero de los que no puede destilarse entrelazamiento puro—.

La destilación del entrelazamiento es importante no sólo para cuantificar el entrelazamiento, sino también para un tipo distinto de corrección cuántica de errores, complementario al uso de los códigos cuánticos de corrección de errores [20, 47, 48]. Supongamos que Alicia y Bob pueden comunicarse clásicamente y que, además, tienen acceso a un canal cuántico con ruido. Alicia desea enviar de manera fidedigna a Bob un qubit desconocido. Si el canal cuántico no tiene demasiado ruido, Alicia puede codificar el qubit input en varios qubits usando un código cuántico de corrección de errores como el de la Fig. 2b, enviarlos a través del canal cuántico para que Bob los descodifique. Sin embargo, este procedimiento no funcionará para canales con mucho ruido, como los que cambian la polarización del 50% de los fotones, ya que tales canales tienen capacidad cuántica cero, $Q = 0$. En este caso, la mejor estrategia conocida es que Alicia no envíe el qubit input a través del canal, sino que prepare varios pares EPR puros y los comparta con Bob usando el canal con ruido (lo que da lugar a pares EPR con ruido); luego, usando su capacidad para comunicarse clásicamente, Alicia y Bob destilan un número pequeño de pares EPR buenos a partir de los pares con ruido y, por último, Alicia usa uno de los pares EPR buenos y comunicación clásica para teleportar a Bob el qubit input de manera segura. La capacidad de la destilación de entrelazamiento de recuperar esos pares EPR da lugar a que, como comentábamos antes, en muchos canales la capacidad cuántica asistida clásicamente Q_2 sea mayor que la capacidad cuántica Q . (Sin embargo, esta ventaja depende de que sea posible la comunicación en ambos sentidos entre Alicia y Bob —si la comunicación está limitada a un sentido, la destilación no es más eficiente que los códigos cuánticos de corrección de errores—). A medida que crece el ruido, un canal cuántico típico pasa por dos umbrales críticos: un umbral de ruido más allá del cual Q se hace cero, pero Q_2 y C siguen siendo positivas, y un umbral crítico más allá del cual Q_2 se hace

cero, pero C sigue siendo positiva.

I. Computación cuántica tolerante a fallos

La CCTF es tanto una generalización de las investigaciones en la teoría del procesamiento de información cuántica, como una necesidad práctica para poder implementar en los laboratorios computaciones cuánticas no triviales. La CCTF moderna ha sido ampliamente descrita (véase la ref. [3] y las referencias que contiene); algunas de sus ideas básicas se resumen en la Fig. 4. Para evitar que un error provoque daños irrecuperables, se utiliza un código cuántico de corrección de errores adecuado para distribuir el estado lógico de manera que se almacene o procese mediante varios qubits físicos, transportados por un conjunto de cables paralelos. Periódicamente, ese conjunto atraviesa una serie de puertas restauradoras R , donde interacciona con qubits ancilla limpios del entorno para corregir los errores, encauzándolos hacia las ancillas que luego se tiran a la basura. Durante el proceso de restauración pueden ocurrir otros errores pero, si no son demasiado numerosos, pueden corregirse en un proceso de restauración posterior (Fig. 4a). Este régimen de restauración activa puede usarse para implementar una memoria cuántica tolerante a fallos, capaz de conservar los estados cuánticos de manera fidedigna durante mucho más tiempo que los tiempos de decoherencia naturales del hardware del cual se ha hecho el conjunto de puertas. Esto es completamente análogo, pero con datos cuánticos en lugar de con datos clásicos, a la memoria de acceso dinámico aleatorio (DRAM, en su acrónimo inglés) que se usa en los ordenadores actuales, en la cual una restauración periódica de la señal sirve para retrasar casi indefinidamente la desaparición de los datos almacenados. Para hacer computación cuántica tolerante a fallos también es necesario, además de almacenar la información, hacer operaciones lógicas sobre ella sin decodificarla de su forma protegida. Para algunas puertas lógicas, como la XOR, esto se puede hacer de manera directa, aplicando la operación sucesivamente a los cables (Fig. 4b). Otras operaciones lógicas, incluyendo algunas rotaciones necesarias de un único qubit, deben hacerse mediante métodos más complicados que conllevan la preparación y prueba de estados entrelazados especiales de un conjunto de qubits auxiliares (ancilla), a los que luego se hace interaccionar con los datos codificados para llevar a cabo la transformación lógica deseada [3].

La esperanza de la computación cuántica reside en el hecho de que, para hacer un cálculo tolerante a fallos de t pasos, sólo hay que multiplicar el número de puertas y cables por un polinomio en $\log t$. Por lo tanto, para cálculos en los que existe una aceleración cuántica significativa, un ordenador cuántico todavía superaría ampliamente a cualquier ordenador clásico para inputs lo suficientemente grandes.

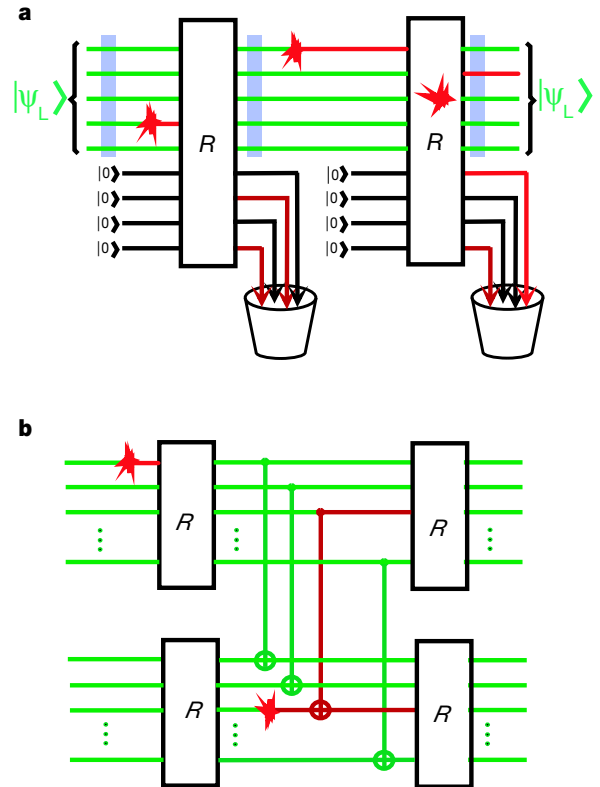


Figura 4: Computación cuántica tolerante a fallos. **a**, Circuito de corrección de errores tolerante a fallos con ancillas nuevas entrando y descartando las corruptas. **b**, Operación XOR sobre datos codificados sin decodificarlos.

J. Criptografía cuántica

Es el arte de aplicar las propiedades únicas de los sistemas cuánticos a propósitos criptográficos, es decir, a la protección de la información clásica frente a la manipulación o revelación no autorizada, en un escenario con muchas partes en el que no todas ellas se fían de las demás. Este elemento antagonista es lo que la distingue de otros tipos de procesamiento cuántico de la información considerados antes.

Un objetivo importante de la criptografía cuántica, la distribución cuántica de claves criptográficas, tiene como propósito que dos protagonistas, Alicia y Bob, compartan una cadena aleatoria secreta K , llamada clave criptográfica, teniendo a su disposición un canal cuántico inseguro y un canal público clásico. (Existen protocolos clásicos para que dos partes acuerden una clave criptográfica y su uso está muy extendido, pero dan como resultado una clave que no es segura desde el punto de vista de la teoría de la información —un adversario con suficiente capacidad de cálculo podría inferirla usando los mensajes públicos que se intercambian Alicia y Bob—. En particular, los protocolos más usados para acordar claves criptográficas podrían romperse fácilmente usando un ordenador

cuántico, si hubiese uno disponible.) En la distribución cuántica de claves está permitido que un espía (Eva) interactúe con los portadores de información cuántica (por ejemplo, los fotones) que están “en ruta” de Alicia a Bob —con riesgo de perturbarlos—, y también puede escuchar pasivamente toda la comunicación clásica entre Alicia y Bob, pero no puede alterar o suprimir los mensajes clásicos. A veces (por ejemplo, si Eva obstruye o interacciona fuertemente con las señales cuánticas), Alicia y Bob detectarán el espionaje y abortarán el protocolo; pero, para cualquier estrategia de espionaje, la probabilidad de que la presencia de Eva no sea detectada y al mismo tiempo Eva obtenga información significativa sobre la clave debe ser despreciable.

La implementación práctica de la distribución cuántica de claves está mucho más avanzada que cualquier otro tipo de procesamiento de información cuántica, debido al hecho de que los protocolos típicos de distribución cuántica de claves no requieren interacciones entre dos qubits, sino sólo la preparación y medida de estados cuánticos sencillos, y comunicación y computaciones clásicas. Se han construido y probado prototipos ópticos que funcionan en decenas de kilómetros de fibra óptica, o incluso al aire libre por la noche hasta una distancia de un kilómetro. En principio, sin embargo, un protocolo cuántico de distribución de claves podría incluir computaciones cuánticas de Alicia y Bob; y, para estar seguros de su inviolabilidad, deberíamos permitir que Eva dispusiese de todo el poder de un ordenador cuántico, incluso en caso de que Alicia y Bob no necesitasen uno para los protocolos típicos.

Se han presentado varias demostraciones de la seguridad de los protocolos cuánticos de distribución de claves, especialmente del protocolo “BB84” de la ref. [49]. Una demostración completa de la seguridad debe abarcar todos los ataques permitidos por las leyes de la mecánica cuántica, y también debe ser capaz de hacer frente al ruido, en la hipótesis realista de que este surja no sólo del espionaje, sino que también es se deba al ruido de los canales y detectores. Por último, debe proporcionar una manera de calcular la velocidad de generación de una clave segura como función de los niveles de ruido observados por Alicia y Bob. Las demostraciones recientes [50, 51], construidas sobre una larga lista de demostraciones de la seguridad frente a ataques más limitados [48, 49, 52, 53], satisfacen ampliamente estos criterios; los problemas que quedan por resolver son: mejorar los umbrales de error, simplificar las demostraciones y extenderlas de manera que cubran el caso de fuentes realistas, que no emiten exactamente estados de un único fotón o pares EPR y que, incluso en casos extremos, pueden haber sido saboteados por Eva.

Tras el éxito de la distribución cuántica de claves criptográficas, había grandes esperanzas depositadas en que las técnicas cuánticas pudieran ayudar a otra tarea, la evaluación inconsciente de funciones entre dos partes (“two-party oblivious function evaluation”), que sería mejor llamar “toma de decisiones prudente”. Esta es la tarea,

que surge frecuentemente en el ámbito del comercio y la diplomacia, que consiste en permitir que dos partes, que desconfían la una de la otra, cooperen en evaluar una función, acordada públicamente, usando datos privados en posesión de cada una de las partes, y sin comprometer los datos privados más de lo que habría sido necesario si esa tarea se hubiese asignado a un intermediario en el que confían las dos partes. Alicia inicialmente conoce los datos x y Bob conoce los datos y ; cuando el protocolo termina, Alicia y Bob también deben conocer $f(x, y)$, pero ninguna de las partes debe conocer nada más del input privado de la otra parte que lo que lógicamente se pueda inferir del conocimiento de sus propios datos y del valor común de la función $f(x, y)$. Existen protocolos clásicos para evaluar inconscientemente funciones entre dos partes pero, como en el caso de los protocolos clásicos de acuerdo de claves, no son seguros y podrían romperse mediante un ordenador cuántico. Las esperanzas de encontrar una base cuántica para una forma segura de evaluación inconsciente de funciones acabaron con el descubrimiento de que un componente fundamental en todos los protocolos de evaluación inconsciente de funciones, llamado compromiso de bits (“bit commitment”) es, en principio, inseguro ante ataques cuánticos [54, 55]. El compromiso de bits es la idealización de un protocolo en el que Alicia envía a Bob una caja cerrada que contiene, escrito en un trozo de papel, un 0 ó un 1 que ella ha elegido; después, cuando ella quiera, le manda la llave de manera que él pueda abrir la caja y leer el bit. El compromiso cuántico de bits es inseguro debido a una propiedad fundamental de los estados entrelazados: si dos estados puros del sistema Alicia-Bob son indistinguibles para Bob, deben ser interconvertibles mediante una acción local de Alicia; por tanto, en principio, no existe ninguna manera de implementar una caja cerrada que contenga un bit que sea tanto inmodificable para Alicia como inobservable para Bob.

Las similitudes y diferencias entre la información cuántica y la clásica se resumen en la Tabla I.

II. ESTUDIOS EXPERIMENTALES DE INFORMACIÓN CUÁNTICA

La continua maduración de la teoría de la información cuántica y la computación cuántica ha estimulado una gran cantidad de trabajos experimentales en una gran variedad de disciplinas, en óptica y óptica cuántica, en investigaciones sobre un solo átomo y un solo ión, y en varias áreas de espectroscopia de precisión. Aquí hablaremos de algunos de los progresos que se han realizado en estos campos. No mencionaremos las muy interesantes perspectivas que se abren al usar tecnología cuántica de estado sólido —puntos cuánticos (“quantum dots”), microcavidades superconductoras, uniones Josephson diminutas y similares— para lograr operaciones tipo puerta lógica cuántica, que aparentemente todavía quedan a varios años en el futuro.

Propiedad	Clásica	Cuántica
Representación del estado	Cadena de bits $x \in \{0, 1\}^n$	Cadena de qubits $\psi = \sum_x c_x x\rangle$
Primitivas de computación	Operaciones booleanas sobre uno y dos bits	Transformaciones unitarias sobre uno y dos qubits
Computación tolerante a fallos	Mediante series de puertas clásicas tolerantes a fallos	Mediante series de puertas cuánticas tolerantes a fallos
Aceleraciones de la computación cuántica		Factorización: aceleración exponencial; búsqueda: aceleración cuadrática; iteración, paridad: no hay aceleración; simulación de sistemas cuánticos: hasta una aceleración exponencial
Primitivas de comunicación	Transmitir un bit clásico	Transmitir un bit clásico; transmitir un qubit; compartir un par EPR
Técnicas de codificación sin ruido	Compresión clásica de datos	Compresión cuántica de datos; concentración de entrelazamiento
Técnicas de corrección de errores	Códigos de corrección de errores	Códigos cuánticos de corrección de errores; destilación de entrelazamiento
Capacidades de un canal ruidoso	Capacidad clásica C_1 que es igual a la máxima información mutua mediante el uso de un único canal	Capacidad clásica $C \geq C_1$; capacidad cuántica no asistida $Q \leq C$; capacidad cuántica asistida clásicamente $Q_2 \geq Q$; capacidad clásica asistida por entrelazamiento $C_E \geq C$
Comunicación asistida por entrelazamiento		Codificación superdensa, teleportación cuántica
Complejidad de la comunicación	Coste de la computación distribuida de comunicar un bit	Coste de un qubit, o coste de un bit asistido con entrelazamiento, puede ser menor
Acuerdo de una clave criptográfica secreta	Los protocolos conocidos son inseguros ante un ordenador cuántico	Seguridad ante ataques cuánticos generales y potencia de cómputo ilimitada
Compromiso de bits entre dos partes	Los protocolos conocidos son inseguros ante un ordenador cuántico	Inseguros ante el ataque mediante un ordenador cuántico

Tabla I: Comparación entre el procesamiento de información clásica y cuántica.

Para implementar muchos de los protocolos de procesamiento cuántico descritos antes serán necesarios “qubits voladores”. Debido a los desarrollos en criptografía cuántica, en la actualidad se producen de manera rutinaria qubits voladores de alta calidad en varios laboratorios. Una innovación importante, introducida por el grupo de Gisin en la Universidad de Ginebra [56], ayuda a hacer posible la transmisión de fotones a través de fibras ópticas de poca fiabilidad. Incluye el uso de un espejo de Faraday, que refleja cualquier luz que incide sobre él con una polarización ortogonal. En su esquema, Bob manda a Alicia un pulso doble de luz en un estado fuertemen-

te coherente mediante una fibra óptica. Alicia lo atenúa hasta la intensidad de un fotón, ajusta la fase relativa de uno de los dos pulsos para obtener uno de los cuatro estados cuánticos del fotón y, por último, refleja este fotón de vuelta a Bob usando el espejo de Faraday. Esta reflexión de Faraday asegura que las distorsiones o variaciones en el modo de propagación de la luz debidas a la birrefringencia (la anisotropía del índice de refracción) en la transmisión de fotones desde Bob a Alicia se deshacen en la transmisión de regreso. Con este invento se logra una notable estabilidad interferométrica: la visibilidad de las franjas de su sistema de transmisión de 23 km

de largo, usado como un interferómetro, es del 99,98%, lo que implica que la fase del fotón es fiable hasta 0,03 radianes. Esto significa que en este sistema se han transmitido satisfactoriamente estados cuánticos de una gran pureza.

La posibilidad de almacenar y procesar qubits usando “qubits quietos” puede aumentar enormemente las capacidades para procesar información cuántica de los “qubits voladores”. Por ejemplo, la posibilidad de hacer conjuntamente computación cuántica y comunicación cuántica mejoraría cualitativamente la posibilidad de hacer criptografía cuántica, permitiendo el uso de repetidores cuánticos y abriendo las puertas a nuevas técnicas para vencer al espionaje, y permitiría también criptografía en distancias arbitrariamente grandes [57, 58]. Con esta idea en mente, algunos investigadores han propuesto un matrimonio entre las técnicas de los sistemas de fotones en fibras ópticas y los sistemas de átomos (o iones) atrapados. En estos esquemas [60, 61], un “qubit quieto”, codificado en el estado de un átomo, se transfiere mediante un pulso láser apropiado [59] a ese mismo estado de un qubit del estado fotónico de una cavidad electromagnética que lo rodea, y desde allí puede convertirse en un “qubit volador”, al escaparse en un modo de propagación en el aire libre o en una fibra óptica. La característica inesperada de este procedimiento se encuentra en el siguiente paso, en el cual el fotón que se propaga afecta a una réplica del sistema emisor. Si se ha tejido adecuadamente el paquete de ondas, puede hacerse que este sistema átomo-cavidad recapture el fotón en el estado atómico mediante una inversión temporal adecuada del procedimiento de emisión.

Aunque algunas extensiones de la demostración original de la puerta lógica de dos qubits usando electrodinámica cuántica en cavidades [62] nos han acercado al propósito de casar los qubits voladores con los qubits quietos, todavía no tenemos un prototipo elemental que funcione. Los experimentos ópticos de electrodinámica cuántica (QED, en su acrónimo en inglés) no han tenido todavía éxito en lograr los estados de dos “qubits quietos”, pero sí se ha logrado entrelazamiento de ese tipo en experimentos en áreas relacionadas, en QED de cavidades de microondas (ref. [63]) y en estudios de iones atrapados [64].

Desgraciadamente, la creación de entrelazamiento controlable con puertas lógicas de dos qubits es sólo uno de una lista formidable de ingredientes que debe tener un experimento para obtener un ordenador cuántico. Hay por lo menos otros cuatro hitos que deben lograrse [66]: (1) El sistema debe ser extensible a un número grande de qubits. (2) Ha de ser posible poner al principio estos qubits en el “0” o estado limpio, de manera fidedigna. (3) La tasa de decoherencia debe ser, como se explicó antes, muy baja (esto es, debe estar por debajo de un umbral adecuado). (4) Debe ser posible hacer medidas únicas de sensibilidad cuántica (si sólo se dispone de un ejemplar del ordenador cuántico) o medidas conjuntas precisas de una manera específica para los qubits (si se dispone de muchos ejemplares del ordenador cuántico).

Un experimento a escala real que cumpla todos estos criterios simultáneamente queda todavía muy lejano. En el campo de la investigación en iones atrapados se están llevando a cabo esfuerzos concertados entre varios grupos experimentales para realizar la propuesta original de Cirac y Zoller [67] para hacer computación cuántica con iones atrapados, que despertó una gran expectación e interés en 1995. La propuesta de estos autores era, ni más ni menos, cumplir todos los requisitos para la computación cuántica mencionados antes: los qubits se representan por estados internos (de espín) de iones individuales mantenidos en una trampa electromagnética; se logra aumentar el número de qubits añadiendo más átomos a la trampa. Las técnicas de enfriamiento por láser (“laser cooling”) servirían para poner el sistema en el estado “0”. El acoplamiento con el entorno en una trampa de iones es pequeño y, por tanto, se ha comprobado que son posibles qubits con unas propiedades razonables de decoherencia. La técnica llamada de espectroscopia de salto cuántico (“quantum-jump spectroscopy”) proporciona la posibilidad de realizar medidas cuánticas únicas con casi un 100% de eficiencia. El núcleo de la propuesta es un esquema detallado para la realización de operaciones cuánticas de dos qubits; su procedimiento conlleva un acoplamiento del estado interno del ión con el estado cuántico de vibración de los iones en la trampa. Debido a que estas oscilaciones implican modos colectivos de todos los iones, resulta posible el entrelazamiento de los estados internos del ión. Desafortunadamente, se ha comprobado que es muy difícil conseguir experimentalmente una de las características del ordenador de Cirac y Zoller —el enfriamiento al estado fundamental del movimiento de la trampa—; este paso esencial sólo lo ha logrado un grupo, y para uno [65] o dos [64] iones.

Aunque las ideas basadas en trampas están en un camino de firme progreso, investigadores en otros campos tienen la lógica esperanza de que sus técnicas les permitan adelantar a los físicos atómicos y ponerse así en cabeza de la “carrera del ordenador cuántico”. Los ponentes de la espectroscopia por resonancia magnética nuclear (RMN), que se practica en química orgánica, han hecho grandes avances en esta dirección. La espectroscopia RMN tiene muchas características útiles para su aplicación en computación cuántica; en el muy estudiado límite en el que las moléculas se agitan rápidamente en una solución, el hamiltoniano de los espines nucleares de la molécula presenta una forma sencilla:

$$H = \sum_i \omega_i \sigma_z^i + \sum_{i,j} J_{ij} \sigma_z^i \sigma_z^j \quad (3)$$

(Aquí σ_z es el operador momento angular de los espines, ω es el desdoblamiento Zeeman, y J es el parámetro de interacción de intercambio.) Este hamiltoniano sólo depende de la componente z de los espines nucleares (aquí indicados como i y j). Un sistema con este hamiltoniano es muy apropiado para la computación cuántica [68, 69]; como conmuta con todos los operadores σ_z^i , todos los estados de la base computacional son autoes-

tados suyos. Por consiguiente, el estado del sistema sólo cambia cuando se aplica un pulso resonante, de manera que la dinámica del sistema está completamente bajo control externo. Seleccionando adecuadamente los tiempos y las frecuencias, un pulso externo puede hacer una operación minuciosamente ajustada, como por ejemplo, voltear un espín i particular si otro espín específico j está hacia arriba; esta es la esencia de la puerta fundamental XOR de dos qubits para computación cuántica. Además, las operaciones de los pulsos pueden hacerse mucho más rápidamente que el tiempo de decoherencia de 1–10 segundos de una molécula elegida adecuadamente. Por último, en una situación en la que se disponga de muchas copias idénticas del ordenador cuántico (la multitud de moléculas idénticas que hay en una solución), la lectura del resultado final se puede lograr mediante una medida colectiva de la magnetización transversal, una operación común en RMN.

Tras las propuestas iniciales de las refs. [70] y [71], ha habido una riada de trabajos sobre sistemas de unos pocos qubits, tan abundante que aquí no haremos más que enumerar brevemente los logros en este área: se ha demostrado la acción de puertas de dos y tres qubits en los protones en 2,3-dibromotiofeno y en 1-cloro-2-nitrobenceno [72]; se han demostrado los algoritmos de Deutsch-Jozsa [73] y Grover [74] usando los espines del H y el ^{13}C en cloroformo; los tres espines H y C del tricloroetileno se han empleado para la síntesis de estados de Greenberger-Horne-Zeilinger [75] para hacer teleportación [37] (ver más arriba) y para simular la acción de un código de corrección de errores de tres qubits [76] (también se han empleado para este último estudio los tres espines C en la alanina); los protones de la citosina también se han empleado para implementar el algoritmo de Deutsch-Jozsa original [77] y asimismo el algoritmo cuántico para contar [78]; y el ácido 2, 3-dibromopropanoico se ha utilizado para algunas secuencias simples de puertas de tres qubits [79].

Los practicantes de la RMN están presionando para implementar más procesamiento de información cuántica en moléculas con un número superior de espines. Sin embargo, para lograr de manera inmediata una computación cuántica a gran escala hay dos grandes obstáculos;

probablemente no sean insuperables, pero pueden hacer que el progreso de la computación cuántica con RMN no vaya más deprisa que en física atómica o en otras áreas. Uno de los problemas es que el rango de frecuencias usadas, en el que cada qubit tiene un desplazamiento químico ω_i , se complica cuando el número de qubits crece mucho. Un segundo problema (que probablemente será la razón más inmediata por la que haya que modificar radicalmente la técnica de RMN para hacer computación cuántica a una escala mucho mayor que 10 qubits) tiene que ver con la preparación de los estados; los estados de espín de las moléculas en una solución que está a temperatura ambiente están distribuidos de una manera casi perfectamente aleatoria, con una pequeña propensión ϵ por el estado cero (típicamente ϵ , que es proporcional a $k_{\text{B}}T$ dividido por la energía Zeeman nuclear, es del orden de 10^{-6}). El número de moléculas en la solución que comienzan en el estado correcto, en lugar de en el estado completamente aleatorio, crece como $\epsilon 2^{-n}$, donde n es el número de espines en la molécula. Por tanto, la fuerza de la señal se vuelve exponencialmente más pequeña con el número de qubits y se pierde toda la ventaja ganada al hacer computación cuántica. Este problema puede resolverse si ϵ puede incrementarse hasta un valor próximo a uno; existen técnicas innovadoras de bombeo óptico que dan esperanzas de que esto se pueda lograr. Aunque hay razones para el optimismo en estos campos, creemos que ello requerirá muchos años de esfuerzo concertado.

Nos viene a la memoria [59] un incidente que se produjo en una conferencia sobre computación cuántica que se celebró en Turín en 1995, cuando Shor apostó a que la primera factorización de un número de 500 dígitos se haría con un ordenador cuántico y no con un ordenador clásico. No hubo nadie que aceptase la apuesta, pero alguien comentó que prefería apostar a una tercera posibilidad: que antes se extinguiría el Sol. Aunque estos escépticos no han sido completamente acallados, en general hoy estamos más de acuerdo con Shor de lo que lo estábamos entonces. Creemos que las posibilidades a favor del ordenador cuántico han mejorado y seguirán aumentando lentamente a medida que disfrutemos de más años de progreso ininterrumpido.

-
- [1] Barenco, A. *et al.* Elementary gates for quantum computation. *Phys. Rev. A* **52**, 3457-3467 (1995).
 - [2] Zurek, W. Decoherence and the transition from quantum to classical. *Phys. Today* **44** (10), 36-44 (1991).
 - [3] Preskill, J. Reliable quantum computers. *Proc. R. Soc. Lond. A* **454**, 385-410 (1998).
 - [4] Shor, P. W. en *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science* 124-133 (IEEE Computer Society Press, Los Alamitos, California, 1994).
 - [5] Ekert, A. y Jozsa, R. Shor's quantum algorithm for factoring numbers. *Rev. Mod. Phys.* **68**, 733-753 (1996).
 - [6] Wiesner, S. Simulations of many-body quantum systems by a quantum computer. Preprint quant-ph/9603028 en <http://xxx.lanl.gov> (1996).
 - [7] Abrams, D. S. y Lloyd, S. Simulations of many-body Fermi systems on a universal quantum computer. *Phys. Rev. Lett.* **79**, 2586-2589 (1997).
 - [8] Grover, L. K. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.* **79**, 325-328 (1997).
 - [9] Boyer, M., Brassard, G., Hoyer, P. y Tapp, A. Tight bounds on quantum searching. *Fortschr. Phys.* **46**, 493-506 (1998).
 - [10] Ozhigov, Y. Quantum computers cannot speed up ite-

- rated applications of a black box. Preprint quant-ph/9712051 en <http://xxx.lanl.gov> (1997).
- [11] Terhal, B. M. *Quantum Algorithms and Quantum Entanglement*. Thesis, Univ. Amsterdam (1999).
- [12] Farhi, E., Goldstone, J., Gutmann, S. y Sipser, M. A limit on the speed of quantum computation in determining parity. *Phys. Rev. Lett.* **81**, 5442-5444 (1998).
- [13] Beals, R., Buhrman, H., Cleve, R., Mosca, M. y de Wolf, R. en *Proceedings of the 39th Annual Symposium on the Foundations of Computer Science* 352-361 (IEEE Computer Society Press, Los Alamitos, California, 1998).
- [14] Jozsa, R. y Schumacher, B. A new proof of the quantum noiseless coding theorem. *J. Mod. Opt.* **41**, 2343-2349 (1994).
- [15] Shor, P. W. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A* **52**, 2493-2496 (1995).
- [16] Calderbank, A. R. y Shor, P. W. Good quantum error correcting codes exist. *Phys. Rev. A* **54**, 1098-1105 (1996).
- [17] Steane, A. Multiple particle interference and quantum error correction. *Proc. R. Soc. Lond. A* **452**, 2551-2577 (1996).
- [18] Knill, E. y Laflamme, R. Theory of quantum error correcting codes. *Phys. Rev. A* **55**, 900-911 (1997).
- [19] Gottesman, D. A class of quantum error-correcting codes saturating the Hamming bound. *Phys. Rev. A* **54**, 1862-1868 (1996).
- [20] Bennett, C. H., DiVincenzo, D. P., Smolin, J. y Wootters, W. K. Mixed state entanglement and quantum error correction. *Phys. Rev. A* **54**, 3824-3851 (1996).
- [21] Helstrom, C. W. *Quantum Detection and Estimation Theory* (Academic, New York, 1976).
- [22] Holevo, A. S. Bounds for the quantity of information transmitted by a quantum communication channel. *Problemy Peredachi Informatsii* **9**, 3-11 (1973); traducido al inglés en *Problems Inf. Transmiss.* **9**, 177-183 (1973).
- [23] Holevo, A. S. Problems in the mathematical theory of quantum communication channels. *Rep. Math. Phys.* **12**, 273-278 (1977).
- [24] Schumacher, B., Westmoreland, M. y Wootters, W. K. Limitation on the amount of accessible information in a quantum channel. *Phys. Rev. Lett.* **76**, 3452-3455 (1997).
- [25] Holevo, A. S. The capacity of the quantum channel with general signal states. *IEEE Trans. Inf. Theory* **44**, 269-273 (1998).
- [26] Holevo, A. S. Capacity of a quantum communications channel. *Problemy Peredachi Informatsii* **15**, 3-11 (1979); traducido al inglés en *Problems Inf. Transmiss.* **15**, 247-253 (1979).
- [27] Sasaki, M., Kato, K., Izutsu, M. y Hirota, O. Quantum channels showing superadditivity in channel capacity. *Phys. Rev. A* **58**, 146-158 (1998).
- [28] Fuchs, C. A. Nonorthogonal quantum states maximize classical information capacity. *Phys. Rev. Lett.* **79**, 1162-1165 (1997).
- [29] Bennett, C. H. *et al.* Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.* **70**, 1895-1898 (1993).
- [30] Bennett, C. H. y Wiesner, S. J. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Phys. Rev. Lett.* **69**, 2881-2884 (1992).
- [31] Bennett, C. H., Shor, P. W., Smolin, J. A. y Thapliyal, A. V. Entanglement enhanced classical capacity of noisy quantum channels. *Phys. Rev. Lett.* **83**, 3081-3084 (1999).
- [32] Mattle, K., Weinfurter, H., Kwiat, P. G. y Zeilinger, A. Dense coding in experimental quantum communication. *Phys. Rev. Lett.* **76**, 4656-4659 (1996).
- [33] Bouwmeester, D. *et al.* Experimental quantum teleportation. *Nature* **390**, 575-579 (1997).
- [34] Boschi, D., Branca, S., De Martini, F., Hardy, L. y Popescu, S. Experimental realization of teleporting an unknown pure quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.* **80**, 1121-1124 (1998).
- [35] Furusawa, A. *et al.* Unconditional quantum teleportation. *Science* **282**, 706-709 (1998).
- [36] Vaidman, L. Teleportation of quantum states. *Phys. Rev. A* **49**, 1473-1476 (1994).
- [37] Nielsen, M. A., Knill, E. y Laflamme, R. Complete quantum teleportation using nuclear magnetic resonance. *Nature* **396**, 52-55 (1998).
- [38] Cleve, R. y Buhrman, H. J. Substituting quantum entanglement for communication. *Phys. Rev. A* **56**, 1201-1204 (1997).
- [39] Buhrman, H., Cleve, R. y Wigderson, A. en *Proceedings of the 39th Annual ACM Symposium on the Theory of Computing* 63-68 (ACM Press, New York, 1998).
- [40] Bennett, C. H., Bernstein, H. J., Popescu, S. y Schumacher, B. Concentrating partial entanglement by local operators. *Phys. Rev. A* **53**, 2046-2052 (1996).
- [41] Lo, H.-K. y Popescu, S. Concentrating entanglement by local actions—beyond mean values. *Phys. Rev. A* **63**, 022301 (2001).
- [42] Vidal, G. Entanglement monotones. *J. Mod. Opt.* **47**, 355-376 (2000).
- [43] Linden, N., Popescu, S. y Sudbery, A. Non-local properties of multi-partite density matrices. *Phys. Rev. Lett.* **83**, 243-247 (1999).
- [44] Thapliyal, A. V. On multipartite pure-state entanglement. *Phys. Rev. A* **59**, 3336-3342 (1999).
- [45] Kempe, J. On multi-particle entanglement and its application to cryptography. *Phys. Rev. A* **60**, 910-916 (1999).
- [46] Horodecki, M., Horodecki, P. y Horodecki, R. Mixed state entanglement and distillation: is there a 'bound' entanglement in nature? *Phys. Rev. Lett.* **80**, 5239-5242 (1998).
- [47] Bennett, C. H. *et al.* Purification of noisy entanglement, and faithful teleportation via noisy channels. *Phys. Rev. Lett.* **76**, 722-725 (1996).
- [48] Deutsch, D. *et al.* Quantum privacy amplification and the security of quantum cryptography over noisy channels. *Phys. Rev. Lett.* **77**, 2818-2821 (1996); **80**, 2022 (1998) (errata).
- [49] Bennett, C. H. y Brassard, G. en *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* 175-179 (IEEE, New York, 1984).
- [50] Mayers, D. Unconditional security in quantum cryptography. *J. ACM* **48**, 351-406 (2001).
- [51] Lo, H.-K. y Chau, H. F. Unconditional security of quantum key distribution over arbitrarily long distances. *Science* **283**, 2050-2056 (1999).
- [52] Griffiths, R. B. y Niu, C.-S. Optimal eavesdropping in quantum cryptography. II. Quantum circuit. *Phys. Rev. A* **56**, 1173-1176 (1997).
- [53] Biham, E., Boyer, M., Brassard, G., van de Graaf, J. y Mor, T. Security of quantum key distribution against all

- collective attacks. *Phys. Rev. Lett.* **78**, 2256-2259 (1997).
- [54] Mayers, D. Unconditionally secure quantum bit commitment is impossible. *Phys. Rev. Lett.* **78**, 3414-3417 (1997).
- [55] Lo, H.-K. y Chau, H. F. Is quantum bit commitment really possible? *Phys. Rev. Lett.* **78**, 3410-3413 (1997).
- [56] Muller, A. *et al.* 'Plug and Play' systems for quantum cryptography. *Appl. Phys. Lett.* **70**, 793-795 (1997).
- [57] Briegel, H. J., Dür, W., Cirac, J. I. y Zoller, P. Quantum repeaters for communication. *Phys. Rev. Lett.* **81**, 5932-5935 (1998).
- [58] Dür, W., Briegel, H. J., Cirac, J. I. y Zoller, P. Quantum repeaters based on entanglement purification. *Phys. Rev. A* **59**, 169-181 (1999).
- [59] Bennett, C. H. y DiVincenzo, D. P. Quantum computing—towards an engineering era? *Nature* **377**, 389 (1995).
- [60] van Enk, S. J., Cirac, J. I. y Zoller, P. Ideal quantum communication over noisy channels: a quantum optical implementation. *Phys. Rev. Lett.* **78**, 4293-4296 (1997).
- [61] van Enk, S. J., Kimble, H. J., Cirac, J. I. y Zoller, P. Quantum communication with dark photons. *Phys. Rev. A* **59**, 2659-2664 (1999).
- [62] Mabuchi, H., Turchette, Q. A., Chapman, M. S. y Kimble, H. J. Real-time detection of individual atoms falling through a high-finesse optical cavity. *Opt. Lett.* **21**, 1393-1395 (1996).
- [63] Haroche, S., Brune, M. y Raimond, J. M. Experiments with single atoms in a cavity: entanglement, Schrodinger's cats and decoherence. *Phil. Trans. R. Soc. Lond. A* **355**, 2367-2380 (1997).
- [64] Turchette, Q. A. *et al.* Deterministic entanglement of two ions. *Phys. Rev. Lett.* **81**, 3631-3634 (1998).
- [65] Monroe, C., Meekhof, D. M., King, B. E., Itano, W. M. y Wineland, D. J. Demonstration of a fundamental quantum logic gate. *Phys. Rev. Lett.* **75**, 4714-4717 (1995).
- [66] DiVincenzo, D. P. y Loss, D. Quantum information is physical. *Superlatt. Microstruct.* **23**, 419-432 (1998).
- [67] Cirac, J. I. y Zoller, P. Quantum computations with cold trapped ions. *Phys. Rev. Lett.* **74**, 4091-4094 (1995).
- [68] Lloyd, S. A potentially realizable quantum computer. *Science* **261**, 1569-1571 (1993).
- [69] Lloyd, S. Envisioning a quantum supercomputer. *Science* **263**, 695 (1994).
- [70] Cory, D. G., Fahmy, A. F. y Havel, T. F. Ensemble quantum computing by nuclear magnetic resonance spectroscopy. *Proc. Natl. Acad. Sci. USA* **94**, 1634-1639 (1997).
- [71] Gershenfeld, N. A. y Chuang, I. L. Bulk spin resonance quantum computation. *Science* **275**, 350-356 (1997).
- [72] Cory, D. G., Price, M. D. y Havel, T. F. Nuclear magnetic resonance spectroscopy: an experimentally accessible paradigm for quantum computing. *Physica D* **120**, 82-101 (1998).
- [73] Chuang, I. L., Vandersypen, L. M. K., Xinlan Zhou-Leung, D. W. y Lloyd, S. Experimental realization of a quantum algorithm. *Nature* **393**, 143-146 (1998).
- [74] Chuang, I. L., Gershenfeld, N. y Kubinec, M. Experimental implementation of fast quantum searching. *Phys. Rev. Lett.* **80**, 3408-3411 (1998).
- [75] Laflamme, R., Knill, E., Zurek, W. H., Catasti, P. y Mariappan, S. V. S. NMR Greenberger Horne Zeilinger states. *Phil. Trans. R. Soc. Lond. A* **356**, 1941-1948 (1998).
- [76] Cory, D. G. *et al.* Experimental quantum error correction. *Phys. Rev. Lett.* **81**, 2152-2155 (1998).
- [77] Jones, J. A. y Mosca, M. Implementation of a quantum algorithm on a nuclear magnetic resonance quantum computer. *J. Chem. Phys.* **109**, 1648-1653 (1998).
- [78] Jones, J. A. y Mosca, M. Approximate quantum counting on an RMN ensemble quantum computer. *Phys. Rev. Lett.* **83**, 1050-1053 (1999).
- [79] Linden, N., Barjat, H. y Freeman, R. An implementation of the Deutsch Jozsa algorithm on a three qubit RMN quantum computer. *Chem. Phys. Lett.* **296**, 61-67 (1998).

Agradecimientos

Este trabajo fue apoyado por la US Army Research office.

La correspondencia y las peticiones de material deben dirigirse a C.H.B. (e-mail: bennetc@watson.ibm.com).